

PROCÉDURE DE DEPLOIEMENT D'UN SERVEUR OPENVPN SUR PFSENSE

Auteur : Maxime GILLE

Reference : Assumer

Date : 07/04/2023



	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSense	Assumer	2 / 14	

DIFFUSION et VISAS

Diffusion				
Société / Entité	Destinataires	Fonction	Diffusion	Pour info
Assumer	Service IT	Procédure	Réseau	

Visas			
Société/Entité	Nom	Fonction	

SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de pages
V1.0	07/04/2023	Maxime GILLE	Procédure d'installation d'un serveur OPENVPN sur PFSense	14

COORDONNEES

Contacts		
Nom	E-mail	Téléphone
Maxime GILLE	maxime.gille@edu.esiee-it.fr	06.43.09.98.54

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSense	Assumer	3 / 14	

Table des matières

1. Topologie réseaux du PFSense

2. Configuration de la solution PFSense page 5

-Créer l'autorité de certification page 5

-Créer le certificat Server page 7

-Créer les utilisateurs locaux page 8

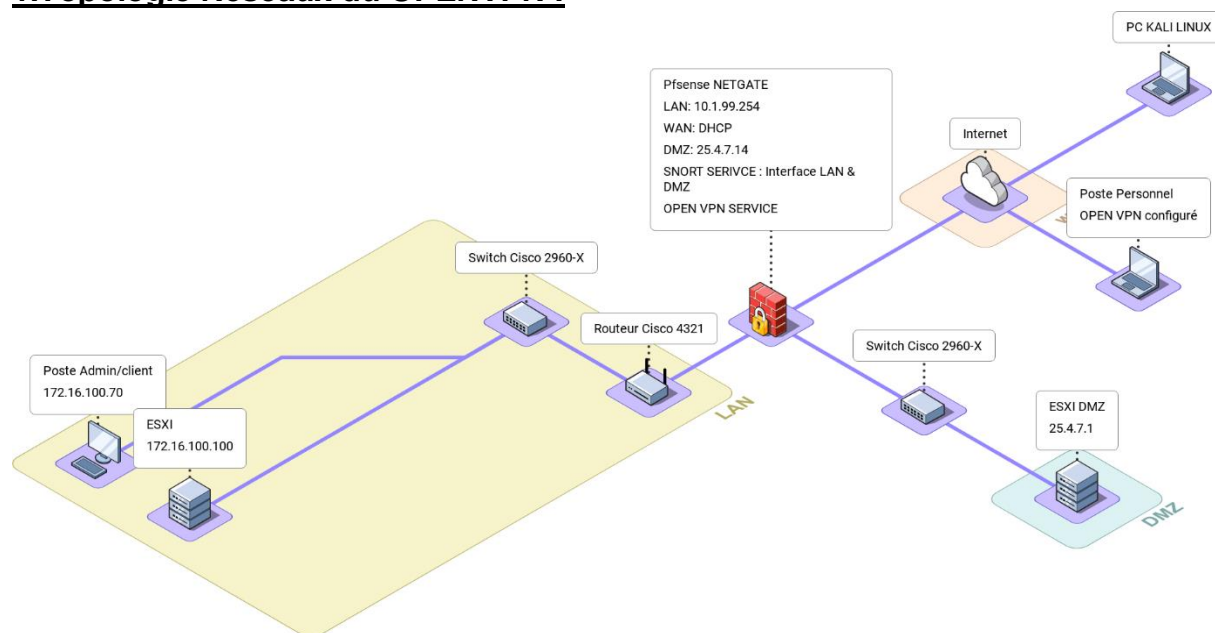
-Configurer le serveur OpenVPN page 9

-Autoriser le flux OpenVPN page 13

-Autoriser les flux vers les ressources page 14

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	4 / 14	

1.Topologie Réseaux du OPENVPN :

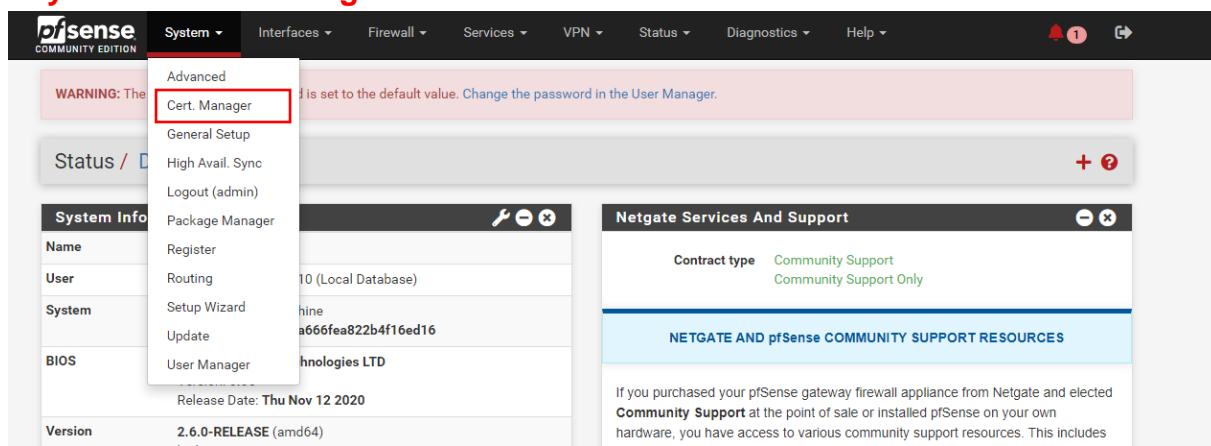


	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	5 / 14	

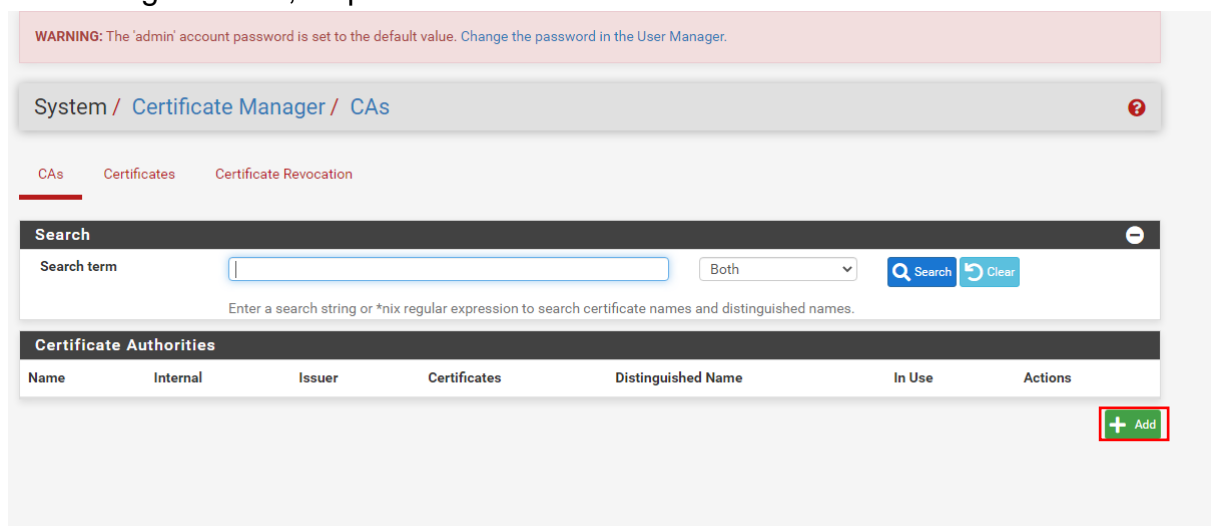
2. Configuration de la Solution PFSENSE :

Créer l'autorité de certification :

Pour créer l'autorité de certification sur **PFSENSE**, vous devez accéder au menu : **System > Cert. Manager**



Dans l'onglet "CAs", cliquez sur le bouton **"Add"**.



	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	6 / 14	

Donnez un nom à l'autorité de certification, Ici "**CA-ASSURMER-OPENVPN**", ce nom sera visible seulement dans Pfsense. Choisissez la méthode "**Create an internal Certificate Authority**".

Concernant le nom qui sera **affiché dans les certificats**, il s'agit du champ "**Common Name**", j'indique "Assumer-VPN". Remplissez les autres valeurs : la région, la ville, etc... et cliquez sur "**Save**" pour créer la CA.

Internal Certificate Authority

Descriptive name: CA-ASSURMER-OPENVPN

Method: Create an internal Certificate Authority

Trust Store: ☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: ☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Key type: RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm: sha256
The digest method used when the CA is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days): 3650

Common Name: Assumer-VPN

The following certificate authority subject components are optional and may be left blank.

Country Code: None

State or Province: e.g. Texas

City: e.g. Austin

Organization: e.g. My Company Inc

Organizational Unit: e.g. My Department Name (optional)

Save

L'autorité de certification doit apparaître dans l'interface, comme ceci :

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-ASSURMER-OPENVPN	✓	self-signed	0	CN=Assumer-VPN Valid From: Fri, 07 Apr 2023 17:50:12 +0000 Valid Until: Mon, 04 Apr 2033 17:50:12 +0000		

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSense	Assumer	7 / 14	

Créer le certificat serveur :

Nous devons créer un certificat de type "Server" en nous basant sur notre nouvelle autorité de certification. Toujours dans "**Certificate Manager**", cette fois-ci dans l'onglet "**Certificates**", cliquez sur le bouton "**Add/Sign**".

System / Certificate Manager / Certificates

CA's Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6406fcd415239) Server Certificate CA: No Server: Yes	self-signed	O=pfsense webConfigurator Self-Signed Certificate, CN=pfsense-6406fcd415239 Valid From: Tue, 07 Mar 2023 08:59:00 +0000 Valid Until: Mon, 08 Apr 2024 08:59:00 +0000		

Choisissez la méthode "**Create an Internal Certificate**" puisqu'il s'agit d'une création, donnez-lui un nom (VPN-SSL-REMOTE-ACCESS) et sélectionnez l'autorité de certification au niveau du paramètre "**Certificate authority**".
Par défaut, la validité du certificat est fixée à 3650 jours soit 10 ans.

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name

Internal Certificate

Certificate authority CA-ASSURMER-OPENVPN

Key type RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days) 3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name e.g. www.example.com

The following certificate subject components are optional and may be left blank.

Country Code None

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	8 / 14	

Choisissez bien le **type de certificat (Certificate Type)** suivant : **Server Certificate**.

Certificate Attributes

Attribute Notes

The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type

Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

FQDN or Hostname

Type

Value





Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add

+ Add

Save

Après avoir cliqué sur **"Save"** pour **valider la création du certificat**, il apparaît dans la liste des certificats du Pare-feu :

VPN-SSL-REMOTE-ACCESS Server Certificate CA: No Server: Yes	CA-ASSURMER-OPENVPN	CN=vpn.assumer.fr Valid From: Fri, 07 Apr 2023 18:07:40 +0000 Valid Until: Mon, 04 Apr 2033 18:07:40 +0000	   
--	---------------------	--	---

Créer les utilisateurs locaux :

Il faut créer **un utilisateur ainsi qu'un certificat de type "User" pour l'authentification VPN**. Pour créer l'utilisateur, il faut indiquer un identifiant, un mot de passe... Ainsi que cocher l'option **"Click to create a user certificate"** : cela va ajouter le formulaire de création du certificat juste en dessous. Pour créer le certificat, on se base sur notre autorité de certification

Certificate

☒ Click to create a user certificate

Create Certificate for User

Descriptive name

Certificate authority

CA-ASSURMER-OPENVPN

Key type

RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

sha256

The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime

3650

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	9 / 14	

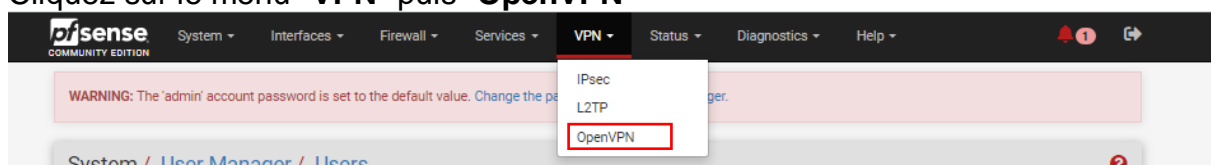
Lorsque l'utilisateur est créé, il apparaît bien dans la base locale :

Users				
	Username	Full name	Status	Groups
<input type="checkbox"/>	admin	System Administrator	✓	admins
<input type="checkbox"/>	assumer.vpn.fr	Maxime ASSURMER	✓	

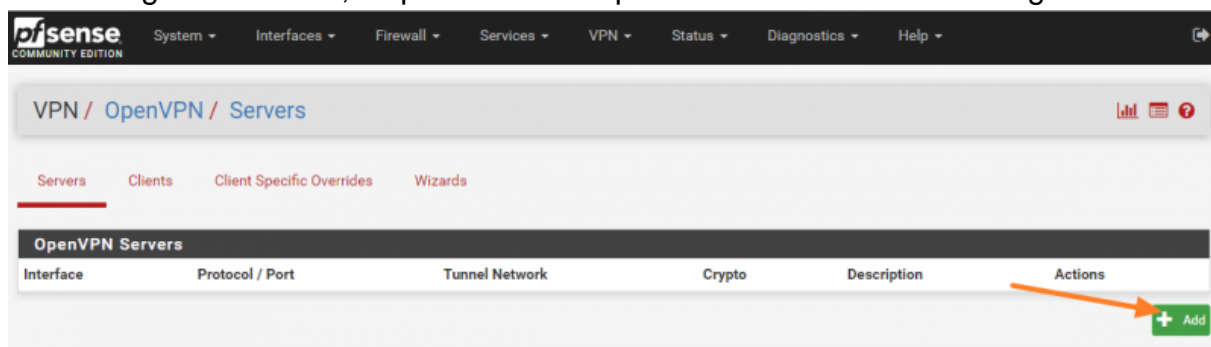
Configurer le serveur OPENVPN :

Maintenant que la partie certificat est opérationnelle et que nous disposons d'un compte utilisateur, on peut s'attaquer à la configuration du VPN.

Cliquez sur le menu "VPN" puis "OpenVPN"



Dans l'onglet "Servers", cliquez sur "Add" pour créer une nouvelle configuration.



	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	10 / 14	

La première chose à faire, c'est de choisir le "**Server Mode**" suivant : **Remote Access (SSL/TLS + User Auth)**.

Pour le VPN, le protocole s'appuie sur de l'UDP, avec **le port 1194 par défaut** : Pour l'interface, nous allons conserver "WAN" puisque c'est par cette interface que l'on va se connecter en accès distant.

General Information	
Description	<input type="text" value="SERVEUR OPENVPN"/> A description of this VPN for administrative reference.
Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.
Mode Configuration	
Server mode	<input type="text" value="Remote Access (SSL/TLS + User Auth)"/>
Backend for authentication	<input type="text" value="Local Database"/>
Device mode	<input type="text" value="tun - Layer 3 Tunnel Mode"/> <small>"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2)</small>
Endpoint Configuration	
Protocol	<input type="text" value="UDP on IPv4 only"/>
Interface	<input type="text" value="WAN"/> The interface or Virtual IP address where OpenVPN will receive client connections.
Local port	<input type="text" value="1194"/> The port used by OpenVPN to receive client connections.

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	11 / 14	

Au niveau de la partie chiffrement, il faut sélectionner votre autorité de certification au niveau du champ "**Peer Certificate Authority**". En complément, sélectionnez le certificat Server au niveau du champ "**Server certificate**".

Cryptographic Settings

TLS Configuration

☒ Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

☒ Automatically generate a TLS Key.

Peer Certificate Authority

CA-ASSURMER-OPENVPN

Peer Certificate Revocation list

No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check

☐ Check client certificates with OCSP

Server certificate

VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: CA-ASSURMER-OPEN)

DH Parameter Length

2048 bit

Diffie-Hellman (DH) parameter set used for key exchange. ⓘ

ECDH Curve

Use Default

The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Negotiation

☒ Enable Data Encryption Negotiation
This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

Data Encryption Algorithms

AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. ⓘ

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	12 / 14	

Passons maintenant à la configuration de notre tunnel VPN en lui-même.

- **IPv4 Tunnel Network** : adresse du réseau VPN, c'est-à-dire que lorsqu'un client va se connecter en VPN il obtiendra une adresse IP dans ce réseau au niveau de la carte réseau locale du PC
- **IPv4 Local network** : les adresses réseau des LAN que vous souhaitez rendre accessibles via ce tunnel VPN25.
- **Concurrent connections** : le nombre de connexions VPN simultanés que vous autorisez

Pour Assumer le réseau VPN sera en **30.30.30.0/24**

Tunnel Settings

IPv4 Tunnel Network

30.30.30.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

☐ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

25.4.7.0

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections

10

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression

Refuse any non-stub compression (Most secure)

Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Push Compression

☐ Push the selected Compression setting to connecting clients.

Dans la zone "**Custom options**", indiquez : **auth-nocache**. Cette option offre une protection supplémentaire contre le vol des identifiants en refusant la mise en cache.

Custom options

auth-nocache




Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	13 / 14	

Validez, le serveur OPENVPN est prêt

ServersClientsClient Specific OverridesWizards

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	30.30.30.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	SERVEUR OPENVPN	  


+ Add

Autoriser le flux OPENVPN :

Cliquez sur le menu "Firewall" > "WAN". Il est nécessaire de créer une nouvelle règle pour l'interface WAN, en sélectionnant le **protocole UDP**.

Edit Firewall Rule	
Action	Pass <small>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</small>
Disabled	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>
Interface	WAN <small>Choose the interface from which packets must come to match this rule.</small>
Address Family	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>
Protocol	UDP <small>Choose which IP protocol this rule should match.</small>

La destination ce sera notre adresse IP publique donc sélectionnez "WAN address". Pour le port, prenez OpenVPN dans la liste.

Destination	
Destination	<input type="checkbox"/> Invert match WAN address Destination Address /
Destination Port Range	OpenVPN (1194) Custom OpenVPN (1194) Custom <small>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</small>
Extra Options	
Log	<input type="checkbox"/> Log packets that are handled by this rule <small>Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).</small>
Description	Autoriser le VPN SSL <small>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.</small>
Advanced Options	 Display Advanced

Validez la création de la règle et appliquez la configuration.

	Titre	Reference	Page	
	Mise en place d'un serveur OPENVPN sur PFSENSE	Assumer	14 / 14	

Autoriser les flux vers les ressources :

Ajoutez une nouvelle règle, cette fois-ci sur l'interface OpenVPN.

La règle qui suit sert à **autoriser l'accès en RDP à l'hôte 25.4.7.1** au travers du tunnel VPN.

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface OpenVPN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol TCP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match Single host or alias 25.4.7.1

Destination Port Range (other) 3389 (other) 3389

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

[Advanced Options](#)

Validez & appliqué, La configuration est terminée.